الأكاديمية للدراسات
الإجتماعية والإنسانية

الصعوبات المادية التي تعترض الإثبات بالمحررات الإلكترونية

رامي علي وشاح
جامعة الجيلالي ليابس – كلية الحقوق – سيدي بلعباس
ramywishah4@hotmail.com

ملخص :

إن الإثبات بالمحررات الإلكترونية المتبادلة عبر الوسائل التكنولوجية الحديثة لا يخلو من صعوبات، مادية أو قانونية، ويختص هذا البحث بدراسة الصعوبات المادية منها.

هذه الصعوبات مرتبطة بمسألتين، الأولى متعلقة بعيوب تعتري أنظمة تشغيل تلك الوسائل التكنولوجية، والمسألة الثانية مرتبطة بأمن البيانات المتبادلة عبر تلك الوسائل.

RESUME :

Le preuve par des moyens technologiques modernes ne manque pas de poser de sérieux problèmes matériels et juridiques. Aussi, cet article se propose de mettre la lumière sur des difficultés pratiques liées essentiellement d'une part aux défauts dans l'utilisation de ces procédés nouveaux et d'autre part aux problèmes se rattachant à la sécurité des informations échangées par le biais de ces canaux.

مقدمة

لقد أوجدت الوسائل التكنولوجية وضعاً يفرض نفسه على الفكر القانوني بإلحاح، الأمر الذي أوجد في نفس الوقت فراغاً ونقصاً في القواعد القانونية المناط بها تنظيم الحجية القانونية الممنوحة للمحررات التي تنتج عن التعامل عبر تلك الوسائل، أو حتى الوسائل التي لا ينتج عنها أثراً مكتوباً.

وما يدفع إلى القول بوجود هذا الفراغ والنقص هو الطبيعة التقنية لهذه الوسائل بالدرجة الأولى، ويعبر عنها بالصعوبات المادية أو الفنية التقنية، فوجود صعوبات فنية أو مادية تجعل من الصعوبة وضع الثقة في تلك الوسائل.

وهي أسباب في الأغلب ترجع إلى الأنظمة التقنية للوسائل المذكورة، هذه الأنظمة – من الناحية القانونية – أنظمة ضعيفة تفتقر إلى وسائل أمان كثيرة، مما يضعف مصداقيتها وبلوغها الشروط المعتبرة قانوناً لاكتساب الحجية الكافية للاحتجاج بها في أي نزاع أو خلاف يثور بشأنها، الأمر الذي أفرز وضعاً يتسم في معظم ملامحه بعجز وقصور القواعد القانونية الحالية عن مواجهة هذه المعضلة.

بالتالي هناك جدل ومعضلة تتعلق بمسألة منح الوثائق الصادرة عبر هذه الأجهزة الحجية القانونية المطلوبة أو الكافية على أقل تقدير.

لذلك توجب التطرق إلى هذه المشكلة والمعضلة عبر محورين، المحور الأول يتناول صعوبة القيام بعملية الإثبات مادياً، أما المحور الثاني فيتطرق إلى الأخطار المتعلقة بالأمن القانوني.

وقد استند البحث إلى المنهج التحليلي القائم على تحليل وشرح طبيعة أنظمة التشغيل التقنية لبعض

الوسائل التكنولوجية محل الدراسة، وتطبيقها على الجانب القانوني الذي يمكن أن يحكم التعاملات عبر هذه الوسائل.

وقد استند البحث إلى دراسة بعض حالات تلك الوسائل على سبيل المثال لا الحصر، لأن الغاية هو الوقوف على العوائق التي تحول دون إقرار الحجية القانونية للمحررات المقصودة، وما لم يذكر من وسائل في هذا البحث لن يبتعد كثيراً عن النقاط التي يثيرها هذا البحث.

وتحليل تلك الصعوبات انطلاقاً من فهم طبيعة عمل تلك الوسائل من الناحية الفنية، ومطابقتها مع الواقع القانوني الموجود بالنصوص القانونية الحالية، حيث تم الرجوع إلى مراجع ومقالات متخصصة أو مراجع قانونية أخذت عن مراجع متخصصة، وفي أحيان أخرى تم الاعتماد على المعرفة الشخصية المقترنة بتجربة فعلية لبعض تلك الوسائل، حيث تم الإشارة إليها في الحواشي بالوسيلة كمرجع (مثال: الحواشي التي تحمل عنوان internet).

لقد تم تقسيم هذا البحث إلى محورين، تطرق المحور الأول يتناول صعوبة القيام بعملية الإثبات مادياً، وتم تقسيمه إلى ثلاث نقطتين الأولى تتناول الصعوبات الناتجة عن أخطار الغش والتدليس، والثانية تتناول صعوبة تحديد هوية المتراسلين، في حين تناول المحور الثاني الأخطار المتعلقة بالأمن القانوني للوسائل التكنولوجية الحديثة، حيث تناول ثلاث نقاط، الأولى تناولت الأخطار المتعلقة بالخطأ، والثانية تتعلق بضعف الأمن القانوني للوسائل التكنولوجية، والثالثة تتعلق بإمكانية حدوث خلل يؤثر على أمن البيانات المتداولة عبر الوسائل التكنولوجية.

وتجدر الإشارة إلى أن هذه الصعوبات لا تواجه كافة الوسائل التكنولوجية المقصودة، بمعني قد توجد هذه الصعوبات والعوائق في وسيلة دون أخرى وقد تلتقي أكثر من وسيلة في عوائق مشتركة، بمعنى أصح لا ينطبق حكم الجزء على الكل، فقد تنفرد وسيلة منها بخصوصية ما دون باقي الوسائل، ولكن اقتضت الضرورة الإشارة إلى أغلب الصعوبات قدر الإمكان، للإحاطة بالموضوع أكثر فأكثر.

الفرع الأول: صعوبة القيام بعملية الإثبات مادياً

وتتعلق هذه الصعوبات بتحديد هوية المتراسلين عبر هذه الوسائل أو المتعاقدين، لأن صعوبة تحديد هويتهم يخلق صعوبة في تحديد أطراف العلاقة القانونية، وما يخلق هذه الصعوبة مخاطر حدوث عمليات الغش أو التدليس، التي تنعكس وتؤثر سلباً وبطريقة غير مباشرة على مسألة تحديد هوية المتراسلين، فتصبح عملية الإثبات منصبة أو موجهة ضد شخص مجهول، بالإضافة إلى الصعوبة المادية المباشرة في تحديد هوية الأطراف.

وسيتم التطرق إلى هذه المسألة عبر نقطتين، وذلك على النحو التالي:

أولاً: الصعوبات الناتجة عن مخاطر الغش والتدليس

تتنوع مخاطر الغش تبعاً لتنوع مصدره، فقد يصدر الغش من المرسل أو من المرسل إليه، كما قد يصدر من الغير؛ أي من طرف خارج عن العلاقة الأصلية كمستخدمي أي من الطرفين.

وما يساعد على زيادة وتنامي هذه المخاطر ضعف الطبيعة التقنية لهذه الأجهزة، والتي تسمح باستعمالها في الكثير من العمليات المتسمة بالغش والتزوير هذا من ناحية، ومن ناحية أخرى فان الطبيعة التقنية لبعض هذه الأجهزة تسمح بإزالة كل أثر أو دليل على حدوث التراسل والاتصال فيما بين المرسل والمرسل إليه.

مثلاً في التعاقد عبر الفاكس يستطيع المرسل تقديم تاريخ الإرسال، كما يمكنه عدم القيام بعملية الإرسال أصلاً مع إمكانية طباعة وصل إشعار الوصول، كونه ورقة منفصلة عن الورقة أو الوثيقة المرسلة،وذلك دون الحاجة إلى القيام بالإرسال فعلاً[1].

كما قد يقوم المرسل – إذا ما التزم تجاه المرسل إليه في إطار صفقة أو التزام ما – بإرسال وثيقتين تتضمن كل واحدة مواصفات وأسعار تختلف كل منها عن الأخرى، ثم يبدأ بالتلاعب بقيمة ومواصفات الالتزام حسب ارتفاع أو انخفاض قيمة أو أرباح الصفقة، بحيث يقدم الرسالة التي تتناسب مع وضعه وحاجته، وعند الاحتجاج عليه يدفع الأصل مناقضاً للوثيقة المرسلة[2].

ونفس الوضع ينطبق على المرسل إليه، إذ يستطيع التلاعب في الوثيقة الواردة بالتحريف في مضمونها سواء بالزيادة أو النقصان، أو حتى بإنكار المضمون كلية، كذلك يمكن للمرسل إليه إنكار وصول أياً من المستندات التي يدعي المرسل إرسالها.

لأنه على الرغم من حيازة المرسل لوصل إشعار الوصول، قد يستند الطرف الثاني إلى أن ذلك الوصل لا يمكن –

بأي حال من الأحوال–اعتباره قرينة قاطعة على صحة الاستلام، لأنه من الممكن تزوير ذلك الوصل وبكل سهولة، وهذا ما دفع بالبعض إلى القول بأن المرسل دائماً يكون في حالة أقل ارتياحاً من المرسل إليه[3].

ونفس العملية قد يقوم بها المرسل إذا ما كان ينوي إرسال رسالة عبر البريد الإلكتروني، إذ يمكنه أن يكتب الرسالة ويتلاعب بمضمونها قبل إرسالها، فيستطيع أن يضمن الرسالة اتفاقاً ما، ويحدد مسبقاً الجزء الذي يريد التلاعب به، ويقوم بطباعة الرسالة، ثم يعدل أو يجري التعديلات التي يريد أن يجريها ثم يعيد المضمون الأصلي الذي يرغب في إرساله.

فهنا تلعب مصلحة المرسل الدور الرئيسي في مضمون الوثيقة التي يمكن له أن يقدمها ويؤيد بها احتجاجه، وتأكيداً لصدق ادعائه.

فهذه عملية ليست صعبة الحدوث إذا ما تم النظر إلى سهولة اختراق النظام التقني الذي تعمل به هذه الأجهزة، فالمرسل إليه – مثل المرسل – يستطيع وبكل سهولة التلاعب في الوثيقة الواردة إليه بتحريف مضمونها بالزيادة أو النقصان أو حتى بإنكار المضمون كليةً.

وكما سبقت الإشارة إليه فإن الغش قد يصدر من عمال أو مستخدمي أي من طرفي العلاقة، هؤلاء يستطيعون أيضاً القيام بكل عمليات الغش والتي يمكن أن يقوم بها المرسل أو المرسل إليه بصفة أصلية، كموظفي البنوك والشركات الكبرى وخصوصاً المكلفين بالعمل على متابعة تلك الاتصالات عبر الأجهزة المخصصة بذلك[5].

وإن كانت هذه الحالة لا تنفي مسئولية المرسل كمسئولية متبوع عن تابعه أو مسئولية حارس الأشياء عن الأجهزة الموجودة في حيازته، إلا أن الحديث هنا لا يدور عن المسئولية بل عن الإثبات وإمكانية التلاعب بالوثائق الصادرة عبر أجهزة الاتصالات الحديثة، سواء كان التلاعب متعلقاً بمضمون الوثيقة أو من حيث وجود تلك الوثيقة من عدمه.

والغش غير قاصر على وسائل الاتصال سابقة الذكر، بل يشمل كذلك الوسائل الصوتية كالتسجيل الصوتي لحوار مباشر أو محادثة هاتفية، فإمكانية دمج وتقليد الأصوات اليوم هي إمكانية واردة وكبيرة ومتاحة، نظراً للتطور التكنولوجي الهائل الذي يسمح بكل سهولة بتقليد وإعادة تركيب الأصوات، بحيث يكون من الصعب جداً كشف تلك العملية بالوسائل المتاحة دون اللجوء إلى وسائل تقنية متطورة[6].

لأن عمليات قص وتركيب حوار كان قد سجل لشخص ما وأعيد تركيبه بحيث تحذف منه بعض المقاطع وتضاف أخرى هو أمر وارد، بحيث يسجل لشخص ما حوار كامل متكامل بشأن التزام ما بتفاصيل معينة، فيعاد قص وتركيب وإعادة التركيب، بحيث يبدو وكأن ذلك الشخص قد التزم بشيء في حقيقة الأمر هو لم يلتزم به بالكيفية التي يظهرها التسجيل.

أما فيما يخص خطر التدليس فيمكن وقوعه بفعل البشر ولا يكون فعل البشر مصدره[7]، ويعتبر هذا الخطر ذو أثر وتأثير كبير النطاق على مجالات الحاسوب كمشكل هام وحيوي، فعملية الغش المعلوماتي أو التدليس تخلف وتتسبب في خسائر مالية معتبرة، إذ بلغت خسائرها في الولايات المتحدة الأمريكية 30مليون دولار وفي اليابان 100 مليون دولار[8].

تجدر الإشارة هنا أن عملية الغش والتدليس هذه قد تقع من موظفي الشركة أو المؤسسة المطلعين على مفاتيح وطرق التشغيل، والذين قد يستغلون وضعهم هذا لتحقيق أغراض شخصية، كالقيام بعملية تحويل رؤوس أموال من حسابات أصحابها إلى أشخاص آخرين.

وقد يحدث ذلك الغش بفعل أشخاص آخرين غير موظفي الشركات الذين يستطيعون بطريقة أو بأخرى الدخول والتدخل في برامج جهاز الحاسوب، خاصة عبر شبكة الاتصالات الرقمية إذ أن نظام الإرسال يسمح بمثل هذا الدخول[9].

ثانياً: صعوبة تحديد هوية المتراسلين

تتمثل هذه المصاعب في عدم المقدرة أو الصعوبة في التعرف على هوية المتراسلين أو المتعاقدين، ذلك أن شخصيتهما تبقى إلى حد ما غير أكيدة هذا من ناحية، ومن ناحية أخرى فإن محتويات العقد في أغلب الأحوال غير مجسدة على ورق ولا موقعة باليد[10].

وهذه في حالة أكثر ما تتضح في وسائل الحاسوب وبالتحديد وسيلة الإنترنت، ويمكن إضافة حالة التيلكس الذي يستحيل – تقنياً – وضع التوقيع على المحررات المرسلة عبره.

فمجرد استخدام الوسائل التكنولوجية للتراسل غير كافٍ

في معظم الأحيان للدلالة على تحديد هوية المتراسلين، وذ لك لاعتبارات تقنية بحتة[11]، فالتراسل عبر الإنترنت سواء بوسيلة البريد الإلكتروني أو منتديات الحوار محفوف بالمخاطر والعقبات، ففي معظم الأحيان يكون العنوان البريدي الإلكتروني لا يحمل اسم صاحبه الحقيقي بحيث لا يوحي إليه على الإطلاق.

لأن مستعملي هذه الوسيلة في – معظم الأحيان – يلجئون إلى استخدام أسماء مستعارة أو جزء من الاسم، ففي هذه الحالة لا يمكن بأي حال من الأحوال التأكد بصورة قطعية ويقينية من هوية المرسل أو المستلم[12]، فمن السهل أن ينكر شخص ما أنه هو من أرسل الرسالة، ويساعده في ذلك أمور كثيرة ، منها عدم إمكانية استرداد الرسالة إذا ما تمت عملية الإرسال[13]، بحيث إذا تم الرجوع إلى بريده لم نجد لها أثراً، هذا من ناحية ومن ناحية أخرى يصعب الحصول على كلمة المرور الخاصة بالشخص المدعى عليه بالرسالة محل الجدل.

كما لا يمكن إجبار ذلك الشخص على تقديمها[14]، بهدف فحص مصدر الرسالة وما إذا كان العنوان البريدي المراد التأكد منه هل هو له أم لا.

فالأمر لا يوحي بإمكانية قطعية نسبة العنوان أو الرسالة إلى الشخص المدعى عليه بها، إضافة إلى أن الرسالة مطبوعة بحروف إلكترونية بحيث يمكن التلاعب بمضمونها بكل سهولة، ناهيك عن إمكانية إنكارها ممن يدعى عليه بها كما يمكن له الطعن فيها بالتزوير أو إنكار صدورها عنه.

لذلك اشترط المشرع الجزائري في المادة 323 مكرر 1 ضرورة التأكد من هوية الشخص الصادر عنه المحرر الإلكتروني، وأن تكون الكتابة محفوظة في ظروف تضمن سلامتها واستمراريتها[15]، كما تصدت المادة 18 من قانون التوقيع الإلكتروني المصري رقم 14 لسنة 2004 هذه المسألة بالإيضاح[16]، وكذلك فعل المشرع البحريني في قانون التجارة الإلكترونية في المادة 6 الفقرات 1 و2 و3 حجية التوقيع الإلكتروني شأنه شأن التوقيع الخطي،ويعتبر صحيحاً – إذا اقترنت به شهادة معتمدة – إلى أن يثبت العكس[17]، ونفس الموقف تبنته التوجيهة الأوروبية المتعلقة بالتوقيع الإلكتروني والصادرة عن مجلس الإتحاد الأوروبي بتاريخ 1999/12/13م في المادة الخامسة[18].

أما موقف المشرع الفرنسي فقد كان واضحاً في المادة (1316.1) التي ساوت بين حجية الكتابة الإلكترونية والكتابة على الورق، بشرط إمكان بيانها للشخص الصادرة عنه وأن تنشأ وتحفظ في أحوال من طبيعتها ضمان اكتمالها أو وحدتها[19].

وليس الحال بأفضل إذا ما كان الحديث يدور عن التراسل بالفاكس، إذ أن وجود رقم فاكس المرسل على الورقة محل النزاع لا يجزم بشأن نسبتها إلى شخص ما بحيث يكون هذا الشخص هو أحد أطراف العلاقة أو العقد.

فالمرسل سيئ النية قد يلجأ إلى استعمال جهاز فاكس غير الجهاز المملوك له تحت ذرائع كثيرة،في هذه الحالة لا يمكن نسبة الوثيقة الواردة إلى ذلك الشخص، وما ينطبق على جهاز الفاكس ينطبق على جهاز الهاتف لنفس السبب تقريباً – وإن كان هناك فارق – ففي كل الأحوال تبقى شخصية المتعاقدين مجهولة إلى حد ما، رغم وجود حالة الهاتف المرئي إلا أن هذه حالة استثنائية ولا يجوز القياس عليها كما لا يجوز تعميم حكمها.

إن الحديث عن هذه المشكلة يدفع إلى الحديث عن مشكلة أكبر، تعتبر نتيجة حتمية لها؛ ألا وهي عملية الاحتيال، لقد انتشرت هذه الظاهرة على المستوى الدولي ؛ بشكل يثير القلق فيما يتعلق بمستقبل التجارة عموماً والدولية منها على وجه الخصوص،وتثور هذه المشكلة ويزداد تفاقمها كلما دار الحديث عن التعاقد عبر وسائل الاتصال الحديثة.

وقد اعتبرت دول العام الثالث بما فيها الدول العربية أكبر ضحية لمثل هذه، العمليات حيث بلغت خسائرها نحو ثلاثة مليارات دولار في العام 1984 فيما يتعلق بالنقل،البحري نتيجة للصفقات تم إبرامها بواسطة هذه الوسائل[20].

وتأخذ أساليب الاحتيال مظاهر عديدة كالتعاقد مع أشخاص أو شركات وهمية لا وجود لها من الناحية القانونية أو المادية حتى، حيث يتم التعاقد على صفقة تجارية بمبلغ وأوصاف معينة ثم يتم التسليم بأوصاف أخرى غير مطابقة البتة لما تم التفاهم عليه،وقد لا يتم التسليم أصلاً.

وتبدو هذه الظاهرة واضحة وجلية عند الحديث عن التعاقد عبر الإنترنت، وخير مثال على ذلك قضية شركةب بابا نويل فرنساب، وتتلخص وقائع هذه القضية في أن أحد متصفحي الإنترنت قد تعاقد مع شركةب بابا نويل

فرنساعبر الموقع التاليwww.Father-Noel.fr، وقام بشراء سلع منها وتبين له بعد تسلمه لها بأنها غير مطابقة للمواصفات التي تم التعاقد مع الشركة على أساسها.

فقام برفع قضية ضدها على أساس الإثراء بلا سبب؛ أمام القضاء الذي قضى بأن شرعية العقد منجزة في جميع نصوصه، وأن الزبون لا يمكن أن يسلم بتأخير ولا يمكن أن يحمل على قبول شيء آخر غير الذي تعاقد عليه[21].

الفرع الثاني : الأخطار المتعلقة بالأمن القانوني للوسائل التكنولوجية

يختلف مصدر هذه الأخطار، فمنها ما يمكن رده أساساً إلى الخطأ، ومنها ما يمكن رده إلى الطبيعة التقنية للوسائل التكنولوجية نفسها، وأياً كان مصدر هذه الأخطاء أو الصعوبات فإن إمكانية وجود مثل هذه الأخطاء يزعزع الثقة في المحررات والوثائق الصادرة عبر هذه الوسائل إلى حد كبير، وهذه الأخطاء تتمثل في :

أولاً : الأخطار المرتبطة بالخطأ

هذه الأخطار متعددة قد يكون مصدرها بشري أو تقني أو يرجع إلى عوامل خارجية، فالأخطار البشرية نادرة الوقوع، وتتمثل في الخطأ الذي يقع من الموظفين أو المكلفين باستخدام الجهاز وذلك عند إدخال المعلومات أو البيانات إلى الجهاز، أو عند القيام بعمليات تحويل رؤوس الأموال من حساب إلى آخر على سبيل المثال.

أما الأخطاء التي تجد أساسها في العوامل الخارجية فهي تتمثل في عوامل البيئة، من رطوبة وحرارة أو تغير في ذبذبات أو شحنات الكهرباء الممونة للجهاز المستعمل، مما ينجم عنه مسح كلي أو جزئي للمعلومات، أو اضطراب في عملية التخزين، ويتعلق مدى حدوث مثل هذه الأخطار من عدمه على مدى نجاعة وفاعلية النظام التقني الذي يتمتع به الجهاز.

والخطأ في هذا المجال قد ينشأ بإحدى طريقتين، الأولى وهي الأكثر اعتيادية، وهي قيام المدعى عليه بتصرف مخالف للقانون، والثانية الأكثر تعقيداً وهي إخلال المدعى عليه بالالتزام بعدم إلحاق الضرر بالآخرين، بمعنى هل التزم معيار العقلانية في عملية برمجة وإدخال البيانات إلى جهاز الحاسوب أم لا[22].

فهناك دائماً مخاطرة أو شك في التشوه الإرادي أو اللاإرادي للمعطيات والمعلومات التي تغذى بها ذاكرات الحاسوب، وهذا في جميع مراحل التعامل مع الجهاز[23]، وأكثر ما يكون مجال هذه الأخطاء هو مجال الشبكات الرقمية، نظراً لوجود عدد كبير من الحواسيب وعدد هائل من المستخدمين، بالإضافة إلى ضعف الوسائل الرابطة لهذه الأجهزة .

ويثور التساؤل الأكثر إلحاحاً ما هي الاحتياطات الواجب أخذها بالحسبان لمنع وقوع مثل هذه الأخطاء، من أجل الوصول إلى تحقيق بنية معلوماتية آمنة ؟

هنا لابد من التحقق وذلك باستخدام كل الوسائل الممكنة والمعقولة لتأمين النظام المعلوماتي من الاستخدام غير المشروع، وذلك بالنظر إلى ما هو مألوف واعتيادي في صناعة التقنيات.

ويتحدد هذا المعيار بتصنيف صناعات التقنيات المختلفة، فإذا كان 80% من الأشخاص يستعملون التقنية (أ)، والعشرين الباقين موزعين بين مستعمل للتقنية (ب)و(ج)، إذن فإن هذا الاستعمال للتقنية (أ)يعني أن استعمالها هي الوسائل الملائمة[24].

وقد بلغت الخسائر الناتجة عن الكوارث المترتبة عن الأ خطاء في فرنسا 11.56 بليون فرنك في عام 1995 مقارنة ب 11.2 بليون في عام 1997[25].

ثانياً : ضعف الأمن القانوني للوسائل التكنولوجية الحديثة

إن هذه الوسائل أصبحت تتسم بالصفة العمومية والعالمية بحيث يتعدى مجال معالجتها حدود التشريعات الوطنية والمحلية[26]، الأمر الذي يتطلب وقفة تشريعية عالمية موحدة، وبالتالي تطرح مسألة الاتفاقيات الدولية التي يمكن لها تنظيم مثل هذه الوسائل بحيث تنعكس هذه الاتفاقيات على التشريعات الوطنية والمحلية.

قبل الحديث عن وجود مثل هذه التشريعات والاتفاقيات لا بد من البحث عن الضمانات الكافية والكفيلة بمنح مثل هذه الوسائل الحجية الكافية واللازمة، وهذا ما يعبر عنه بفكرة الأمن القانوني.

وبناءً على ما تقدم يمكن القول بأن فكرة الأمن القانوني يمكن تعريفها على أنها المعايير والمواصفات التي يجب أن تتوفر في الوسائل التقنية التعاملاتية بحيث تجعل من هذه الوسائل محل اعتبار واعتراف من طرف القانون.

فمشكلة الأمن القانوني يزداد طرحها يوما بعد يوم تزايداً مرافقاً لتطور هذه الوسائل التكنولوجية، مثلما هو الحال في الكتابة الإلكترونية، على خلاف الكتابة على ورق رغم عدم خلو هذه الأخيرة من أية مخاطر[27].

فأدلة الإثبات الورقية ليست بمنأى عن الخطر مقارنةً مع الأدلة الكتابية التكنولوجية، والأمر بينهما يتعلق بصعوبة ومخاطر التغيير، فالكتابة على ورق هي جزء من تراث قديم لا يمكن التخلي عنه مرة واحدة، على الرغم أن التزوير في الأدلة التكنولوجية يحتاج إلى أشخاص متمرسين، فهي إذن أقل خطورةً من مثيلتها الورقية[28].

وتطرح كذلك بصدد مسألة التوقيع الإلكتروني الذي هو مناط التعبير عن الإدارة فيستوجب أن تقوم الثقة على أن التوقيع لصاحبه وليس لشخص آخر قلده، فحسب ما يوحي به مصطلح الأمن القانوني من دلالة يمكن القول أنه يتوجب وضع ضوابط قانونية من أجل إضفاء الحجية المطلوبة على الوثائق أو التعاملات عبر هذه الوسائل.

فالقانون هو إطار اجتماعي ينظم العلاقات الفردية والجماعية، فهو ليس بمعزل عن هذه الوسائل وليس بمنأى عنها، ولا يرفض بتاتاً إعطائها الحجية الكافية للاعتراف بها كوسائل معتمدة في الإثبات[29].

ولكن في الوقت ذاته لا يمكن منحها الحجية القانونية بطريقة عشوائية، فهذه الوسائل بوضعها الحالي ليست بمنأى عن الضرر أو الخطر، إذ قد يحدث وأن تتعرض ذاكرتها أو برامجها وأنظمة تشغيلها التقنية إلى خطأ أو عطل (سواء متعمد أو غير متعمد)، ينشأ عن هذا الخطأ إصابة هذه الوسائل والأجهزة بفيروسات، قد تتسبب في إزالة أو محو كلي أو جزئي للمعلومات والبيانات الواردة فيها أو بواسطتها[30].

هذا الأمر يثير مشكلة أخرى أكثر تعقيداً من مشكلة الأمن القانوني؛ ألا وهي مشكلة تحديد التزوير واكتشافه ووسيلة إثباته[31]، وخير مثال على ذلك مجال السرقة والقرصنة المعلوماتية التي أكثر ما تجد مجالها في البنوك وتحويل الأموال من بنوك إلى أخرى، أو في إطار نفس البنك؛ ولكن من حسابات أشخاص إلى حسابات أشخاص آخرين، وذلك بطريقة يصعب معها تحديد الخطأ، وفي بعض الأحيان حتى اكتشافه يكون أمراً في غاية الصعوبة[32].

الأمر يزداد تعقيداً في هذا المجال بعد يوم في ظل تنامي وتزايد ظاهرة أصبحت تعرف بظاهرة قطاع الطرق الإلكترونيين أو قراصنة المعلومات، مما يزيد من تعقيد وتصعيب دور رجال القانون يوما بعد يوم، الأمر الذي يسمح بالقول أنه أمام مثل هذه المعطيات فإن القانون اليوم يقف عاجزاً عن التصدي لمثل هذه الظواهر.

ثالثاً: إمكانية حدوث خلل ما يؤثر على أمن البيانات

وهذه مسألة واردة بحسب الطبيعة التقنية والفنية لوسائل الاتصال خاصة والوسائل التكنولوجية بصفة عامة، إذ قد يحدث وأن تتأثر البيانات والمعلومات المتناقلة بواسطتها إلى خلل قد يؤدي إلى مسح جزئي أو كلي لتلك البيانات؛ نتيجة لضعف برامج تشغيل تلك الأجهزة أو بسبب إصابة ذاكراتها بفيروسات تؤثر على أدائها.

وعلى الرغم من أن اصطلاح أمن المعلومات وان كان استخداماً قديماً سابقاً لولادة وسائل تكنولوجيا المعلومات، إلا أنه وجد استخدامه الشائع بل والفعلي في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال، بل ربما أمسى أحد الهواجس التي تؤرق مختلف الجهات[33].

ويعبر عن مصطلح أمن البيانات بالأمور التالية :

1 – السرية أو الموثوقية : بمعني أن تكون البيانات المتداولة عبر الأجهزة التكنولوجية في مأمن من أن تكون عرضة لإطلاع الغير عليها،وبالتحديد الأشخاص غير المخولين بالإطلاع عليها

2 – التكاملية وسلامة المحتوى : ويقصد بها أن تكون تتم عمليات نقل المعلومات والبيانات قد تمت بطريقة سليمة، وأن محتوى تلك البيانات لم يتعرض لا للتحريف ولا للتشويه ولا للعبث به خلال مراحل النقل والمعالجة، سواء في مرحلة التعامل الداخلي مع المعلومات، أو عن طريق تدخل غير مشروع .

3 – استمرارية توفر المعلومات أو الخدمة : التأكد من استمرار عمل النظام المعلوماتي، واستمرار تقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات سيكون بوسعه في أي وقت الدخول والإطلاع على تلك البيانات أو المعلومات.

4 – عدم إنكار التصرف المرتبط بالمعلومات ممن قام به : ويقصد به ضمان تحديد الشخص الذي قام بتصرف ما متصل بالمعلومات وسد الطريق على أي محاولة من

جانبه لإنكار قيامه بالتصرف.

وآخر ما يمكن الحديث عنه في مسألة أمن البيانات هي النطاق أو الحيز المادي لأمن البيانات، ويتحدد أمن البيانات بالأوجه التالية :

1 – أمن الاتصالات : ويراد بأمن الاتصالات حماية المعلومات خلال عملية تبادل البيانات من نظام إلى آخر.

2 – أمن الكمبيوتر : ويراد به حماية المعلومات داخل النظام بكافة أنواعها وأنماطها كحماية نظام التشغيل و حماية برامج التطبيقات وحماية برامج إدارة البيانات وحماية قواعد البيانات بأنواعها المختلفة[34].

وقد تنبهت الكثير من التشريعات إلى مسألة أمن البيانات عندما عالجت مسائل التكنولوجية الحديثة، لا سيما مسألة التوقيع الإلكتروني ومدى توافر وسائل وعناصر الأمن المطلوبة فيه، ومن هذه التشريعات القانون المصري في اللائحة التنفيذية للقانون رقم 14 لسنة 2004 المتعلق بالتوقيع الإلكتروني في المادة 2 من اللائحة المذكورة والتي حددت الضوابط والمعايير الأمنية القانونية الواجب توافرها من الناحية – الفنية والتقنية – لاعتبار التوقيع الإلكتروني آمناً وذو مصداقية[35].

خـــاتـمـــة :

كما تبيين فإن الثورة التكنولوجية لم تترك مجالاً في حياتنا إلا وطرقته، ولم يستثنَ منها حتى أمور الحياة اليومية والمعيشية، ولم يعد بإمكان القانون كنظام يحمي ويعالج كل أمور الحياة أن يبقى بعيداً عن مثل هذه المتغيرات.

فبدأ هنا الصراع الحتمي بين القانون بمتطلباته وبين طغيان هذه الثورة التكنولوجية على شتى مناحي الحياة، فبدأ الحديث يدور عن إبرام العقود والمعاملات عبر هذه الوسائل، لما لها من ميزات توفر الجهد والوقت والنفقات، غير أن هذا يأتي على حساب أمور أخري تتطلب في كثير من الأحيان الروية والتريث، وأهم هذه المسائل ألا وهي إثبات مثل هذه التعاملات.

أي التزام أو حق يحتاج إلى البرهان أو الدليل على وجوده، فطبيعة هذه الوسائل تثير إشكاليات تعيق من الناحية القانونية منح الحجية القانونية المطلوبة، فالسؤال المطروح كيف يمكن التغلب على مثل هذه المشكلة ؟.

فالأمر لا يخلو من تقصير تشريعي؛ لا يخص مشرع بذاته دون الآخر، فقد أغفل المشرعين هذه الثورة المخيفة في عالم التكنولوجيا – وإن لم يكن هذا الإغفال عمداً – بحيث تسللت إلى شتى مناحي الحياة وأصبحت الخطوات التشريعية تلحق بهذه التطورات بخطى لاهثة.

الأمر الذي أحدث فجوة بين الأنظمة القانونية السائدة أو ما يمكن تسميتها التقليدية، وبين الأنظمة القانونية التي بدأت تأخذ جسماً وإطاراً يلحق بوصف التكنولوجيا، فأصبحت مسألة تعديل بعض القوانين أو بعض النصوص لا يكفي في أغلب الأحيان، لأن الأمر يمتد ليمس قوانين أخرى، بل وأحياناً يتعارض مع قوانين لدول أخرى إذا ما دار الحديث عن مسألة تنازع القوانين من حيث المكان.

تـوصـيــــات :

الحل ليس بالسهولة التي يمكن تصورها، وليس بالصعب المستحيل، ولكن يمكن إيجازه في عدة نقاط :

– ضرورة تضافر الجهود القانونية والتكنولوجية بحيث يساير القانون ويتتبع هذه الاختراعات منذ بدايتها، والوقوف على برامج تشغيلها وأنظمة عملها، وليس الانتظار حتى تصبح شائعة الاستعمال ثم يبدأ العمل لسن القوانين والتشريعات لتنظيمها.

– وضع تشريعات دقيقة تراعي خصوصية ودقة هذه التقنيات من ناحية، ووضع قواعد قانونية مرنة بالقدر الذي يسمح أو يسهل عملية ضبط التعاملات عبرها، وفي ذات الوقت ليس على حساب المبادئ الثابتة في القوانين الموجودة.

– ضرورة تضافر الجهود القانونية والجهود التقنية الفنية للوصول إلى أفضل مستوى وقدر من الأمن القانوني الذي ينبغي أن تتمتع به هذه الوسائل.

– يمكن القول بأنه يتوجب إعطاء سلطة تقديرية ومرنة للقاضي؛ بحيث يستطيع تغطية القصور الذي قد يعتري النصوص القانونية التي قد يتم تشريعها أو سنها، لكون القاضي أقرب من المشرع في معرفة ومعالجة احتياجات أفراد المجتمع، وبحكم أن النظام العام القضائي أكبر وأشمل من النظام العام التشريعي، كون أن مهمة الأول تطبيق القانون بهدف تحقيق العدالة، ولا تقتصر مهمته على تطبيق التشريع، فالفرق شاسع ما بين المصطلحين هذا من جهة.

– وجوب خلق قضاء متخصص – وظيفياً – في النزاعات

التي تنشأ بخصوص التعاملات التي يتم إبرامها بواسطة هذه التقنيات من جهة أخرى، فلا يعقل أن ينظر القاضي في نزاعات من هذا القبيل دون أن يتمتع بتكوين يؤهله على الأقل لفهم الطبيعة التقنية لهذه الوسائل التكنولوجية .

– ضرورة تضافر وتوحيد الجهود على المستوى الدولي لضبط الأمور وإحكام السيطرة على الفراغ القانوني الذي يعصف بهذه المسألة، لأن الأمور تتخطى حدود الدولة الواحدة، وإن كانت هناك جهود حثيثة في هذا الشأن تم التعبير عنها بعدة اتفاقيات دولية، منها قانون الأونسيترال النموذجي الخاص بالتجارة الإلكترونية وآخر خاص بالتوقيع الإلكتروني والصادرين عن الجمعية العامة للأمم المتحدة، وكذلك التوجيهة الأوروبية الصادرة عن الإتحاد الأوروبي المتعلقة بالتوقيع الإلكتروني وملاحقها.

الـهــــوامــش :

(1) Benoit DUTOUR, Convention et preuve et télécopieurs, Recuil Dalloz, 2000, page. 16; L. LAUTRETE, téléx, telécopoie, télegramme, valeur juridique et force probante, Les Pitites Affiches,10 Mai 1996.page. 7.

(2) Benoit DUTOUR, op. cit, page. 17; Jerome HUET, la valeur Juridique de telecopie (ou fax) comparee au telex, Recuil Dalloz siery,1992,page.35.

(3)Jerome HUET, op.cit,page.35.

(5) وخير مثال على ذلك قيام مكتب التحقيقات الفيدرالية الأمريكية المعروف بال F.B.I بإلقاء القبض على ثلاثة أشخاص من ضمنهم أحد العاملين في شركة لبرامج الكمبيوتر المزودة للبنوك بالنظام التقني لبطاقات الدفع المصرفية، وقاموا – بمساعدته – بالحصول على معلومات لبطاقات بنكية لأكثر من 30000 شخص خلال الفترة الممتدة من 1991 حتى2001 ، وقد وصفت هذه الجريمة بأنها أسهل قضية سرقة في تاريخ الولايات المتحدة الأمريكية في هذه القضية : د.حسني عبد الصبور، سلبيات التوقيع الإلكتروني، الأهرام الاقتصادي، العدد 1772 الصادر بتاريخ 2002/7/23م، ص 39.

(6) د. رضا المزغني، أحكام الإثبات، مطابع معهد الإدارة العامة، المملكة العربية السعودية، الطبعة الأولى1985 ،ص 316.

(7) Bernard AMORY et Y. POULLET, Le droit de la preuve face à l'informatique et à la télématique : Approche de droit comparée, Droit L'informatique& télécom,DOCTRINE.1988, page 11.

(8)Bernard AMORY et Y. POULLET, op. cit, page 12.

(9) د. محمد حسام لطفي ،استخدام وسائل الاتصال الحديثة في التفاوض على العقود وإبرامها، طبعة 1988، ص 41.

(10) Michel Jaccard, Problèmes juridiques liés à la sécurité des transactions sur le réseau, page 2, consultable en ligne sous : htpp//www.signelec.com

(11) Eric A. CAPRIOL, La securite Technique et la cryptology dans la commerce électronique en droit Francaise, page 3, consultable en ligne sous : http// www.lex-electronica.org.

(12) Cedric MANARA& Tino ROSSI, Les risques Juridiques liès à internet,consultable en ligne sous : www.juriscom.net.

(13)Internet.

(14) كون ذلك يتنافى مع المبدأ العام في الإثبات القاضي بعدم جواز إجبار الشخص على تقديم دليلاً ضد نفسه.

(15) والتي تنص على : يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها.

(16) حيث نصت على : يتمتع التوقيع الالكتروني والكتابة الالكترونية والمحررات الالكترونية بالحجية في الإثبات إذا ما توافرت فيها الشروط الآتية :

أ) ارتباط التوقيع الالكتروني بالموقع وحده دون غيره.

ب) سيطرة الموقع وحده دون غيره على الوسيط الالكتروني.

ج) إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الالكتروني أو التوقيع الالكتروني.

(17) 1 – لا ينكر الأثر القانوني للتوقيع الإلكتروني، من حيث صحته وإمكان العمل بموجبه، لمجرد وروده – كلياً أو جزئياً – في شكل إلكتروني .

2 – إذا أوجب القانون التوقيع على مستند، أو رتب أثرا قانونيا على خلوه من التوقيع، فإنه إذا استعمل سجل إلكتروني في هذا الشأن، فإن التوقيع الإلكتروني عليه يفي بمتطلبات هذا القانون.

3 – إذا عرض بصدد أية إجراءات قانونية توقيعَ إلكتروني مقرون بشهادة معتمدة، قامت القرينة على صحة ما يأتي ما لم يثبت العكس أو يتفق الأطراف على خلاف ذلك :

أ – أن التوقيع الإلكتروني على السجل الإلكتروني هو توقيع الشخص المسمى في الشهادة المعتمدة.

ب – أن التوقيع الإلكتروني على السجل الإلكتروني قد وضع من قبل الشخص المسمى في الشهادة المعتمدة بغرض توقيع هذا السجل الإلكتروني.

ج – أن السجل الإلكتروني لم يطرأ عليه تغيير منذ وضع التوقيع الإلكتروني عليه.

(18) حيث نصت الفقرتين الأولى والثانية على :

1 – يجب علي الدول أن تؤكد أن التوقيعات الإلكتروني المتطورة التي تستند علي شهادة موصوفة والتي يتم إنشائها بواسطة أداة توقيع آمنة، تفي بتحقيق المتطلبات القانونية لارتباط التوقيع الإلكتروني بالبيانات المتخذة شكل الإلكتروني، بذات الطريقة التي يحققها التوقيع بخط اليد بالنسبة للبيانات الواردة علي الورق.

2 – تلتزم الدول بتأكيد أن التوقيع الإلكتروني المتطور والمنشأ بأداة تأمين إنشاء التوقيع والذي يؤيده شهادة موصوفة، لا يجد فاعليته القانونية أو الاعتراف به كدليل في المرافعات القانونية تأسيسا علي أنه متخذاً شكلاً إلكترونياً أو أنه غير مستند على شهادة غير موصوفة أو انه لا يستند علي شهادة موصوفة صادرة من مقدم معتمد لتقديم إصدار تلك الشهادات أو انه علي ينشأ بأداة مؤمنة لإنشاء توقيع مؤمن.

وهذا هو نص الفقرتين باللغة الفرنسية :

1. Les États membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature :

a) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier.

b) soient recevables comme preuves en justice.

2. Les États membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que :

- la signature se présente sous forme électronique.

- qu'elle ne repose pas sur un certificat qualifié.

- qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification.

- qu'elle n'est pas créée par un dispositif sécurisé de création de signature

(19) Article. 1316-1. - L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conserve dans des conditions de nature à en garantir l'intégrité.

(20) د. سمير المنقبادي، التداول الإلكتروني لوثائق النقل البحري، مجلة الأكاديمية العربية للنقل، العدد 29 فيفري 1990، ص23.

(21) Tribunal de Grand instance de Lyon, Chambre des urgences, 28 mai 2002, consultable en ligne sous : www.juriscom.net.

(22) Nicolas VERMEYS, «Computer Insecurity» And Viral Attacks : Liability Issues Regarding Unsafe Computer System Under Quebec Law page 2. consultable en ligne sous : www.lex-electronica.org

(23) Hervé CROZE, Informatique, preuve et sécurité, Recuil Dalloz siery, 1987, 24eme CAHIER - CHRONIQUE, page 166 ; Jean-Mauriee OUDOT, La signature numerique, Les Pitetes Affiches, 6 MAI 1998 N° 54, page 36.

(24) Nicolas VERMEYS, op. cit, page 3.

(25) المقدرة بواسطة CLUSIF نادي امن الكمبيوتر الفرنسي انظر :

Eric A. CAPRIOL ; La securite Ticnique et la cryptology dans la commerce electronique en droit Francaise op. cit. page 5.

(26) Eric A.CAPRIOLI, Signature Electronique La Loi Française sur la preuve et la signature électroniques dans la perspective européen Dir 1999/93 CE DU parlement européen et du conseil du13 Décembre 1999, La Semaine Juridique Edition General 2000, page.787.

(27) Pierre - Yves GAUTIER, le bouleversement du droit de la preuve : vers un mode Alternatif de Conclusion des conventions, Les Petites Affiches, 7 FEVRIER, 2000, page 6.

(28) د. رضا متولي وهدان، الضرورة العملية للإثبات بصور المحررات في ظل تقنيات الاتصال الحديثة – دراسة مقارنة، دار النهضة العربية، القاهرة، طبعة 1997، ص 61.

(29)André LUCAS, Le droit de L'informatique, Esses uneversitairs de France, 1ere edition 1987, page 371.

(30) وهذا الفيروس عبارة عن برنامج أيضا يصممه بعض المخربين ويتم إدخاله في نظام وسائل الاتصال وخاصة الحسابات الإلكترونية في مجال البنوك. د. طاهر الشيخ، فيروسات الحاسب الإلكتروني وتأثيرها على أمن البيانات في البنوك، صحيفة الأهرام المصرية، عدد 39788 السنة 120، بتاريخ 1995/11/13.

(31) د. سميحة القليوبي، القانون لا يعرف الفاكس، تحقيق الأهرام تحقيق الأهرام المصرية، أجراه أيمن مهدي، السنة ال 118 عدد 39185 في 1994/03/20.

(32) د. رضا متولي وهدان، مرجع سابق، ص57.

(33) أمن البيانات من زاوية أكاديمية هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تقنية، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، ومن زاوية قانونية، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت)، المحامي. يونس عرب، أمن المعلومات ماهيتها وعناصرها وإستراتيجيتها، ص1، مجموعة عرب للقوانين، على الموقع : www.arablaw.org.

(34) المحامي يونس عرب الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي، مجموعة عرب للقوانين، مرجع سابق، ص 22.

(35) حيث نصت المادة 2 من اللائحة التنفيذية المذكورة على : تكون منظومة تكوين بيانات إنشاء التوقيع الإلكتروني مؤمنة متى استوفت ما يأتي :

أ) الطابع المتفرد لبيانات إنشاء التوقيع الإلكتروني.

ب) سرية بيانات إنشاء التوقيع الإلكتروني.

ج) عدم قابلية الاستنتاج أو الاستنباط لبيانات إنشاء التوقيع الإلكتروني.

د) حماية التوقيع الإلكتروني من التزوير، أو التقليد، أو التحريف، أو الاصطناع أو غير ذلك من صور التلاعب، أو من إمكان إنشائه من غير الموقع.

ه) عدم إحداث أي إتلاف بمحتوى أو مضمون المحرر الإلكتروني المراد توقيعه.

و) ألا تحول هذه المنظومة دون علم الموقع علما تاما بمضمون المحرر الإلكتروني قبل توقيعه له.

في حين نصت المادة 3 على : يجب أن تتضمن منظومة تكوين بيانات إنشاء التوقيع الإلكتروني المؤمنة الضوابط الفنية والتقنية اللازمة، وعلى الأخص ما يلي:

أ) أن تكون المنظومة مستندة إلى تقنية شفرة المفتاحين العام والخاص وإلى المفتاح الشفري الجذري الخاص بالجهة المرخص لها والذي تصدره لها الهيئة، وذلك كله وفقاً للمعايير الفنية والتقنية المشار إليها في الفقرة (أ) من الملحق الفني والتقني لهذه اللائحة.

ب) أن تكون التقنية المستخدمة في إنشاء مفاتيح الشفرة الجذرية لجهات التصديق الإلكتروني من التي تستعمل مفاتيح تشفير بأطوال لا تقل عن 2048 حرف إلكتروني (bit).

ج) أن تكون أجهزة التأمين الإلكتروني (Hardware Security Modules) المستخدمة معتمدة طبقا للضوابط الفنية والتقنية المشار إليها في الفقرة (ب) من الملحق الفني والتقني للائحة.

د) أن يتم استخدام بطاقات ذكية غير قابلة للاستنساخ ومحمية بكود سرى، تحتوى على عناصر متفردة للموقع وهى بيانات إنشاء التوقيع الإلكتروني وشهادة التصديق الإلكتروني، ويتم تحديد مواصفات البطاقة الذكية وأنظمتها ، وفقا للمعايير الفنية والتقنية المبينة في الفقرة (ج) من الملحق الفني والتقني للائحة.

ه) أن تضمن المنظومة لجميع أطراف التعامل إتاحة البيانات الخاصة بالتحقق من صحة التوقيع الإلكتروني، وارتباطه بالموقع دون غيره، وأن تضمن أيضا عملية الإدراج الفوري والإتاحة اللحظية لقوائم الشهادات الموقوفة أو الملغاة وذلك فور التحقق من توافر أسباب تستدعى إيقاف الشهادة، على أن يتم هذا التحقق خلال فترة محددة ومعلومة للمستخدمين حسب القواعد والضوابط التي يضعها مجلس إدارة الهيئة.